Exhibit 10 to Declaration of Mark C. Mao ISO Plaintiffs' Unopposed Motion for Final Approval of Class Action Settlement

Note: This doc is focused on potential workarounds of the options laid out below. Any policy proposal or statement is not covered here, and still needs to be fleshed out. Any policies that are focused on for Newton, will be up-leveled to the expected outcome, instead of any of these specific mechanisms to enforce the policy.

[redacted]

What are the privacy workarounds that the ecosystem could employ?

@hjun @wanggang, @nitish, @deepakr, @jasonh. @cbindra

[redacted]

January 20th, 2019

Purpose of this doc: Listing the various work arounds that players within the ads ecosystem might be able to employ if 3P ccokies are banned entirely (Option 3) or if 3P cookies are reset every N days (Option 1C)

Background

ACM 1/18/2019

- Option 1: Shepherd the ecosystem slowly, while focusing on the user
- Option 1C: Auto reset 3p cookies and provide users options over reset cycle
- Option 3: Google disables all cross-site personalized. Ads + Chrome bans 3P cookies, and creates no monetization alternative

Overview

This doc describes work-arounds that AdTech vendors can take when either Option 3 or Option 1C gets implemented.

Work-arounds to No 3P Cookie (Option 3)

Deals outside of Open Auctions

Who: large publishers

How: Large publishers may make deals with advertisers to deliver Ads Campaigns, targeting based publishers' data, e.g., contextual, geo, language, and user interests.

- Direct sales: publishers negotiate with advertisers offline and set up delivery through DFP or other publisher platform. Almost no rev share.
- programmatic guaranteed and private marketplace deals (new-york-times): PG (programmatic guarantees), PD (preferred deals)

How to prevent:

- Sustain publisher's revenue
- Unlike Direct sales, moving to PG and PG is positive directions for Google as well due to higher price than OA.

Fingerprint

Who: Any AdTech vendors whose privacy bar is low.

How:

- Use information available to create a unique identifier of the user, regardless of visiting domains.
- For example, based on the k-anonymity analysis over RTB callouts,
- IP address + UA (user agent) can reveal individual user with high probability.
- Javascript running in top level domain can call various browser API to collect more signals.

How to prevent:

- Fuzzify IP address, UA, and other signals that can potentially identify users by combined together.

Sign-in

Who: Any AdServer that provides signed-in; FB, Amazon, Google, etc.

How: use a round of ping and 1P cookie storage or other storage of browser to store signed-in id (or ID mapped to signed-in id) in encrypted form (e.g., using per-pub encryption key).

How to prevent: NA

Sign-in Consortium (German News pubs)

Who: Publishers, advertisers and other AdTech Vendors participating in a consortium

How:
When a user signs in with a publisher or an advertiser, the publisher gets *a registered consortium user id* and stores it in 1P cookie (or memory of a browser). It can be passed along with ad requests or conversions.

How to prevent: NA

Work-around to Resetting 3P Cookies (Option 1C)

AdTech vendors can use one of the following mechanisms to map between old and new 3P cookies.

3P IDs in 1P cookie jar

Who: Any AdTech vendors, who have permission to run JS in the top level domain on a publisher's page, can add a cookie to the 1P cookie jar.

How:
While Chrome browsers reset 3p cookies, AdTech vendors can keep the mapping between 1P cookie and 3P cookies over time. For example,

- 1P cookie A -> 3P Cookie 1

- 1P cookie A -> 3P Cookie 2

Now they can tell 3P Cookie 1 and 2 are for the same user.

This is how the GFP cookie works for AdManager.
Similar work-around can be done on header bidding through Prebid.js

How to prevent: resetting 1p cookies at the same time may disallow this workaround. However, it will affect publishers' organic usage of 1P cookies.

Signed-in identifiers

Who: Any AdServer that provides signed-in; FB, Amazon, Google, etc.

How:
Either advertiser or publisher allows FB pixel on the page to fire a ping.
The ping can be used to set FB 3p cookie on the browser under fb.com.
Later when a user goes to fb.com and signs into FB, FB can create a mapping between 3P cookie A and signed-in ID.

After Chrome browser resets 3P cookies, FB can have another mapping between new 3P cookie and FB signed-in ID.

- FB signed-in id A -> 3P Cookie 1
- FB signed-in id A -> 3P Cookie 2

Now they can tell 3P Cookie 1 and 2 are for the same user.

How to prevent: regulation, ToS or policy demands not to join signed id with pseudo id (signed-out cookies)

Fingerprinting

Who: Any AdTech vendors whose privacy bar is low.

How: Calculate FP based on IP + User Agent and use it as persistent identifiers.

- FP -> 3P Cookie 1
- FP -> 3P Cookie 2

Therefore, they can tell 3P Cookie 1 and 2 are for the same user.

How to prevent: remove unique information as much as possible, e.g.,

- Fuzzify IP address, User Agent (UA), and other signals that can potentially identify users by combined together.

Device IDs, IMEI

Who: Any AdTech vendors

How:

Click pings can be used to map between Mobile Device ids and mobile browser ids ([redacted] in DVA). That is, impression happened on App, but a click opens a browser while conveying device id in clickstring.

Even after 3P cookie reset, the mapping can be created.

- Device id -> 3P Cookie 1
- Device id -> 3P Cookie 2

Now they can tell 3P Cookie 1 and 2 are for the same user.

How to prevent: When opening a browser from a click on ads on mApp, open only Webview browsers, which is not the main browser, so the main browser's cookies won't be linked together. This solution only works with the support from Ads SDK vendors who control whether to navigate to the landing page in main browser or webview.

There is a backdoor which assigns a unified identity for all Webview browsers. However, it will still use a different Jar from the main browser.

Joining permanent identifiers

The story would be similar to fingerprint scenario. However, I am not aware of any other permanent identifiers from web traffic other than fingerprint from ip address and other signals.

Who: Any publishers and advertisers working together with ad tech vendors

How:
Publishers/advertisers asks for users' email addresses (or other PII), then pass the email addresses to ad tech vendors together with the ad tech vendors' 3p cookie.

Even after 3P cookie reset, the mapping can be created.

- Email address -> 3P Cookie 1
- Email address -> 3P Cookie 2

Now they can tell 3P Cookie 1 and 2 are for the same user.

How to prevent:

ID consortia

Who: Ad tech companies team up to form various ID consortia.

How:
Compared to individual ad tech company solving their own ID issues independently, ID consortia can solve all members' ID issues in a much scalable and economical way. For example,

1. An ID Consortium typically shares a centralized ID with all consortium members, therefore, avoiding the cookie matching cost and inefficiency among consortium members.
2. An ID Consortium will likely have direct integration with publishers and advertisers. The ID Consortium's tag run in publisher/advertiser's top level domain, therefore has access to 1p cookie.

The ID Consortium synchronize 1p cookie and 3p cookie once after 3p cookie reset, completely defeats the purpose of 3p cookie reset for all Consortium members.

3. An ID Consortium can join 3p cookies across reset via PII, as long as any member obtains PII information (for example, a news site that asks users to register with an email address to read articles for free). Such a solution wouldn't be scalable, practical or economical for small ad tech companies

How to prevent: Regulation, ToS, policy.

Carrier ID

Who: ad tech companies affiliated with, or are subsidiary of wireless carrier, e.g. AppNexus is a subsidiary of AT&T.

How:
Wireless carriers know the true identity of their subscribers. Even for HTTPS requests from smartphones, wireless carriers know how to bill the smartphone owner for bandwidth consumption. Wireless carriers can share the true identity of their subscribers with affiliated ad tech companies for ads personalization, measurement and spam detection.

How to prevent: Regulation. It is not clear whether wireless carrier will honor users' opt-out settings in Operating System or in browser.

More Frequent Cookie Match

What: The immediate outcome of frequent 3p cookie auto-reset will lead to lower cookie match rate across the industry, which directly lead to lower efficiency in programmatic buying on the web.

Who: ad tech companies

How:
The immediate response from ad tech companies would be to increase the cookie matching pixels dropped right after 3p cookie auto-reset. Such solution may help ad tech companies to reach reasonable cookie match rate with minimum engineering cost.

Such solution allows websites to track and collect user data more frequently than status-quo, in a process completely opaque to Internet users. It reduces user privacy protection. Furthermore, more cookie matching pixels slow down page rendering, increases bandwidth and battery consumption for mobile devices.

How to prevent: Regulation. Policy. ToS.